AN3429
Application note

STM32 proprietary code protection overview

Introduction

Software providers are developing complex middleware solutions (Intellectual Propriety (IP) code), which needs to be protected.

This IP code must be available as a plug-in in the end-user applications to build the complete solution. The global protection mechanism limits access to it via a dedicated application programming interface (API), while preventing any read access.

This application note provides an overview of the mechanism used to protect proprietary code from possible read out by the end-user code, debugger tools or RAM Trojan code. This mechanism provides a full API so the IP code can be easily called by the end-user application and still be protected against direct access to the IP code itself.

The proposed solution is based on the MPU features and a special memory and peripheral management mechanism from the end-user application and the IP code.

In the STM32 proprietary code protection method, two levels of protection are used:

- Global Read Out Protection (Global ROP): IP code and end user code are protected against direct reading (by debugger tools or RAM Trojan code) through STM32 ROP.
- IP code Read Out Protection (IP ROP): IP code protected against end user code (possible Trojan code) through the MPU.

As, once the global ROP is activated, the user no longer has full control of the Flash for programming, the primary application (IP code) must also embed an IAP Layer. This IAP allows loading the end-user application without compromising the protected code area.

For more details about the complete solution, please contact your local ST sales representative.

Contents

1 Code protection overview 3

2 Revision history 4

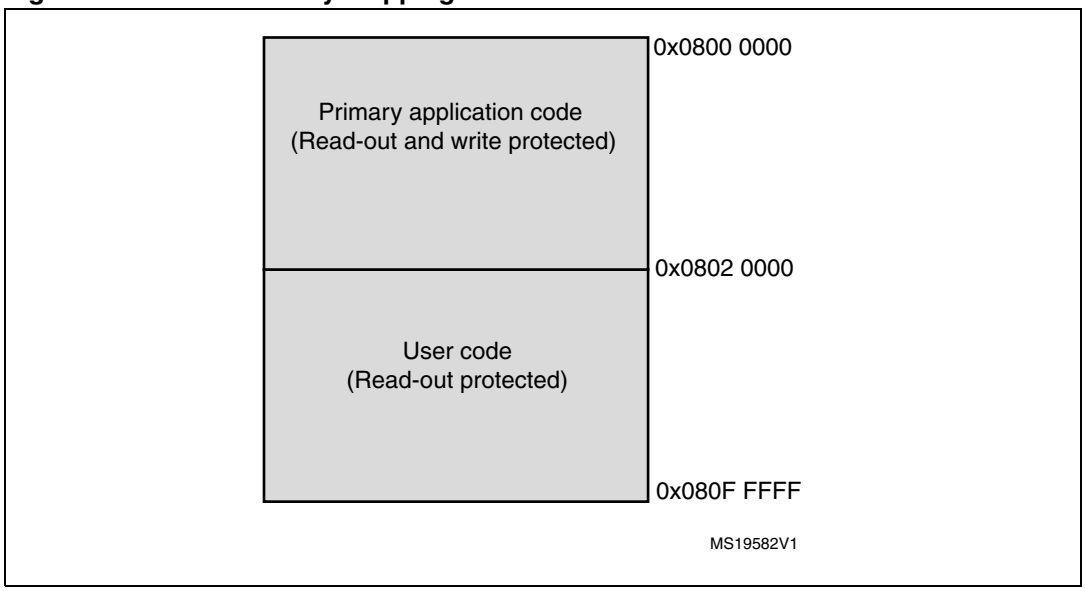
1 Code protection overview

The Flash is divided into two main areas:

- Primary application code: contains the IP memory protection code, the IP code to be protected and the IAP code that enables the loading of the end-user application.
- User code: contains the end-user application and uses the primary system application API offered by the IP memory protection code to provide access to the IP code in protected mode.

Figure 1 shows an example of Flash memory mapping (STM32F2 family)

Figure 1. Flash memory mapping



The IP Code is starts at address 0x0801 0000 defined in the linker file as follows:

```
define region IP_CODE_region = mem:[from 0x08010000 size 0x10000];
place in IP_CODE_region   { section IP_Code };
```

In this example the functions to be protected are forced-loaded in the IP code section using the following pragma with IAR:

```
#pragma location="IP_Code"
(Function definition)
```

The end user project uses the *exported_api.h* file that contains the IP code APIs of the function used by the end user application.

2 Revision history

Table 1. Document revision history

Date	Revision	Changes
19-Jul-2011	1	Initial release.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY TWO AUTHORIZED ST REPRESENTATIVES, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER’S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

© 2011 STMicroelectronics - All rights reserved

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com